Приложение № 12 к приказу
ГАПОУ «ОГК»
от 28.02.2022г. № 115

Требования к защите персональных данных реализуемые ГАПОУ «ОГК»

1. Государственное автономное профессиональное образовательное учреждение «Оренбургский государственный колледж» (далее – Оператор) обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»; Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; нормативными правовыми актами, принятыми Федеральной службой по техническому и экспортному контролю.

2. При обработке персональных данных Оператор принимает необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Обеспечение безопасности персональных данных достигается, в частности, посредством:

определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработки моделей угроз;

применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

проведения оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

организации учета машинных носителей персональных данных;

обнаружения фактов несанкционированного доступа к персональным данным и принятия мер по их недопущению;

восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установления правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

контроля над принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

4. В целях обеспечения безопасности персональных данных, обрабатываемых без использования средств автоматизации, в отношении каждой категории персональных данных Оператором определяются места хранения персональных данных (материальных носителей) и устанавливается перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. Оператором обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Оператором.

6. В целях исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при обработке персональных данных в информационных системах, Оператор использует средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

7. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Классификация информационных систем персональных

данных осуществляется Оператором в порядке, установленном законодательством Российской Федерации.

8. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

9. Персональные данные, обрабатываемые в информационных системах, могут быть представлены для ознакомления:

должностным лицам Оператора, допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей;

уполномоченным лицам, осуществляющим обработку персональных данных по поручению Оператора на основании заключенного с ним договора;

уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

Должностные лица, доступ которым к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных обязанностей, допускаются к соответствующим персональным данным на основании утвержденного Операторам списка.

10. При обнаружении нарушений порядка предоставления персональных данных Оператор приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

11. В целях реализации, эксплуатации, контроля и поддержания на должном уровне системы обеспечения информационной безопасности Оператором назначено должностное лицо, ответственное за организацию обработки Оператором персональных данных, за выполнение законодательных требований при их обработке, за обеспечение информационной безопасности Оператора.